ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT



УДК 512.6
DOI 10.23947/1992-5980-2018-18-2-246-255

Геометрическая реализация метода проведения электронных выборов, основанного на пороговом разделении секрета*

А. В. Мазуренко[1], В. А. Стукопин[2]**
[1]ООО «ДДОС-Гвард», г. Ростов-на-Дону, Российская Федерация
[2]Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Geometric realization of electronic elections based on threshold secret sharing***

A. V. Mazurenko, V. A. Stukopin**
[1]DDoS-GUARD LLC, Rostov-on-Don, Russian Federation
[2]Don State Technical University, Rostov-on-Don, Russian Federation

Введение. Среди актуальных задач криптографии можно выделить задачу обеспечения безопасного и честного проведения электронного голосования. В настоящей работе описан метод проведения электронных выборов с точки зрения обеспечения криптографической безопасности.
Материалы и методы. При решении поставленной исследовательской задачи использованы теоретические результаты из теории конечных полей, проективной геометрии и линейной алгебры. Разработанная криптосистема основана на применении геометрических объектов, рассматриваемых в проективной геометрии над конечными полями.
Результаты исследования. Разработанный алгоритм основан на схеме шифрования Эль-Гамаля и на новом геометрическом способе разделения секрета между избирательными комиссиями. Данный способ использует особенности построения аффинных пространств над конечными полями для создания подходящих геометрических конструкций и генерации секрета, поиск которого, с точки зрения злоумышленника, является сложной алгоритмической задачей. Использование порогового метода разделения секрета обосновывается необходимостью исключить возможность фальсификации результатов голосования со стороны членов избирательной комиссии. Авторами определено, с какой вероятностью злоумышленнику удастся сгенерировать верную секретную долю в случае, когда ему известна лишь ее некоторая часть.
Обсуждение и заключения. Предложенная криптографическая система может быть применена для проведения электронных выборов, а также в тех областях, где возникает необходимость в использовании методов пороговой криптографии.

Introduction. One of the tasks arising in cryptography is to ensure a safe and fair conduct of e-voting. This paper details the algorithm of electronic elections particularly that part which deals with the cryptographic security.
Materials and Methods. The results are obtained on the basis of the following methodology: finite field theory, projective geometry, and linear algebra. The developed cryptosystem is based on the application of geometric objects from projective geometry over finite fields.
Research Results. The invented algorithm relies on the ElGamal encryption and a new geometric way of secret sharing among election committees. The proposed method uses some features of affine spaces over finite fields to generate special geometric constructions and secret, search of which is a complex algorithmic task for an illegal intruder. The threshold secret sharing is used to prevent voter fraud on the part of the members of election committees. The probability to generate the right share of secret by an illegal intruder in case when he/she knows only a part of secret shares is determined.
Discussion and Conclusions. The described scheme is useful for electronic voting and in other spheres where methods of threshold cryptography are applied.

Ключевые слова: криптография, криптосистема с открытым ключом, схема Эль-Гамаля, конечные поля, пороговая криптография, разделение секрета, аффинная геометрия, проективные пространства, электронные выборы, задача Диффи-Хеллмана.

Keywords: cryptography, public-key cryptosystem, ElGamal encryption system, finite fields, threshold cryptography, secret sharing, affine geometry, projective spaces, electronic voting, Diffie-Hellman problem.



Образец для цитирования: Мазуренко, А. В. Геометрическая реализация метода проведения электронных выборов, основанного на пороговом разделении секрета / А. В. Мазуренко, В. А. Стукопин // Вестник Дон. гос. техн. ун-та. — 2018. — Т. 18, № 2. — С. 246–255. DOI 10.23947/1992-5980-2018-18-2-246-255

For citation: A.V. Mazurenko, V.A. Stukopin. Geometric realization of electronic elections based on threshold secret sharing. Vestnik of DSTU, 2018, vol. 2, no.2, pp. 246–255. DOI 10.23947/1992-5980-2018-18-2-246-255

Введение. Авторами разработана криптосистема, основанная на пороговом разделении секрета, которую возможно применить при разработке протокола электронного голосования. Для шифрования и дешифрования голосов используется усиленная схема Эль-Гамаля. Согласно данной схеме генерируется некий секретный параметр, далее называемый секретом, являющийся элементом определенной циклической группы. Для разделения секрета между проверяющими авторами разработан способ, заключающийся в следующем: секрету взаимно однозначно ставится в соответствие некоторая прямая аффинного пространства, ассоциированного с векторным пространством k^n над конечным полем k, где $n \in \mathrm{N}$. Это аффинное пространство будем считать объемлющим пространством для всех рассматриваемых геометрических объектов. Далее проводится некоторая фиксированная плоскость через эту прямую. Эта плоскость объявляется каждому из проверяющих. Затем строится некоторое аффинное подпространство *M*, размерность которого совпадает с количеством проверяющих, и выделяется семейство подпространств, вложенных в *M* и образующих полный флаг. При этом *M* должно удовлетворять следующему свойству: результатом его пересечения с «публичной» плоскостью является в точности «секретная» прямая, причем данная прямая не лежит ни в каком собственном подпространстве, принадлежащем построенному семейству подпространств *M*. Итак, в качестве секретных долей используются попарно различные аффинные прямые, лежащие в аффинном подпространстве *M*, так что их число совпадает с размерностью *M*, а сами они порождают *M*. Для восстановления секрета необходимо найти прямую сумму секретных долей, что позволяет восстановить аффинное подпространство *M*, пересечение которого с «публичной» плоскостью дает «секретную» прямую, соответствующую в силу построенной биекции искомому секрету. Обладая секретным ключом, проверяющие могут расшифровать, согласно схеме Эль-Гамаля, голоса избирателей и в дальнейшем подвести итог голосования. В данной работе в качестве геометрии, при помощи которой будут реализованы описанные идеи, выбрана проективная геометрия.

На сегодняшний день существует множество работ, посвященных вопросам проведения электронного голосования. Многие из них нашли применение в странах, где такое голосование широко используется.

Данная работа носит исключительно теоретический характер и относится скорее к области алгебры и ее возможных приложений, при этом не претендуя на полноту изложения с точки зрения криптографии.

Постановка задачи. Построим криптосистему, основанную на пороговом разделении секрета [1], для обеспечения легитимных электронных выборов [2–5]. Можно выделить три стороны, которые будут участвовать в моделируемом процессе: администратор, проверяющие и избиратели. Администратор — доверенное лицо, которое обладает наибольшими полномочиями и является аналогом центра сертификации.

Представляет интерес задача создания таких условий, при которых ни один из проверяющих не был способен самостоятельно расшифровать шифротекст, представляющий собой результат голосования некоторого избирателя. В общем случае потребуем, чтобы для дешифрования потребовалось участие *t* проверяющих, где $1 < t$.

Основная часть. В работе будут использоваться следующие стандартные обозначения: N — множество натуральных чисел, $\langle X \rangle$ — линейная оболочка подмножества *X* некоторого линейного пространства *V*, $Ord(R)$ — порядок произвольной группы *R*, A^T — транспонированная матрица для матрицы *A*.

Предположим, что общее количество проверяющих $z = Nt$, где $z, N \in \mathrm{N}$. Пусть $S = \{s_1, s_2, \ldots, s_z\}$ — множество проверяющих. Разделим их на команды из *t* человек. Пусть далее S_i обозначает *i*-ю команду, где $i = \overline{1, N}$, состоящую из определенных *t* проверяющих, то есть $S_i = \{s_{i1}, s_{i2}, \ldots, s_{it}\}$, $\bigcup_{i=1}^{N} S_i = S$, $S_i \cap S_j = \varnothing$, где $i \neq j$, $i, j = \overline{1, N}$. Предположим, что все необходимые параметры генерирует администратор, за исключением оговоренных случаев.

В основе разработанной криптосистемы лежит усиленный вариант схемы Эль-Гамаля [6–8]. Согласно данной схеме, по известному алгоритму генерируются параметры (p, g), где *p* — простое число, а *g* —

порождающий элемент мультипликативной абелевой группы $G \subset Z_p^*$, причем порядок $Ord(G) = q$, где q — такое простое число, что $q = (p-1)/2$. Пара (p, g) объявляется частью открытого ключа.

Этап генерации секретного ключа. Сначала при помощи некоторого генератора псевдослучайных чисел необходимо получить случайное число $x \in \overline{1, q-1}$, принимаемое в качестве секретного ключа. Опишем разработанный метод, позволяющий разделить x на секретные доли, которые раздадут каждому из проверяющих.

Пусть $s \in \mathrm{N}$, r — некоторое простое число, $m \in \mathrm{N}$: $t \le m$. Обозначим проективное пространство размерности m над полем Φ_{r^s}, индуцированное векторным пространством $\Phi_{r^{s(m+1)}}$ над полем Φ_{r^s}, через $PG(m, r^s)$ или $PG(\Phi_{r^{s(m+1)}})$ [9]. Пусть $PG(m, r^s)$ состоит из множества точек, однородные координаты которых определяются как $(a_0 : a_1 : \ldots : a_m)$, $a_i \in \Phi_{r^s}$, $\exists$ $j \in \overline{0, m}$: $a_j \ne 0$. Всего в $PG(m, r^s)$ существует $\left(r^{(m+1)s} - 1\right)/\left(r^s - 1\right) = 1 + r^s + r^{2s} + \ldots + r^{ms}$ различных точек.

Положим далее, что $w = r^s$, α — примитивный элемент поля $\Phi_{w^{m+1}}$, $\beta = \alpha^n$ — примитивный элемент поля Φ_w, где $n = \left(w^{m+1} - 1\right)/\left(w - 1\right)$, а также $q < w^{m+1}$, где, как было указано выше, $x \in \overline{1, q-1}$. Легко увидеть, что верна

Лемма 1. Рассмотрим множество $A = \{\alpha^0, \alpha^1, ..., \alpha^{n-1}\}$, где $n = \left(w^{m+1} - 1\right)/\left(w - 1\right)$. Тогда для всех α^i, $\alpha^j \in A$, $i \ne j$, выполняется условие $\alpha^i \ne \gamma\alpha^j$, где $\gamma \in \Phi_w^*$, $i, j \in \overline{0, n-1}$.

Рассмотрим векторное пространство $\Phi_{w^{m+1}}^{w-1}$ над полем Φ_w. Выделим подпространство

$$L = \{\bar{0}\} \cup \left\langle \left(\alpha^0, \beta\alpha^0, \ldots, \beta^{w-2}\alpha^0\right), \ldots, \left(\alpha^i, \beta\alpha^i, \ldots, \beta^{w-2}\alpha^i\right), \ldots, \left(\alpha^{n-1}, \beta\alpha^{n-1}, \ldots, \beta^{w-2}\alpha^{n-1}\right) \right\rangle$$

векторного пространства $\Phi_{w^{m+1}}^{w-1}$ над полем Φ_w, где $i \in \overline{0, n-1}$, $n = \left(w^{m+1} - 1\right)/\left(w - 1\right)$. Заметим, что $dim(L) = m + 1$. Действительно, L содержит $n(w-1) + 1 = w^{m+1}$ точек. Тогда $dim(L) = log_w w^{m+1} = m + 1$. Рассмотрим разбиение D множества $L \setminus \{\bar{0}\}$, определяемое семейством множеств: $A_i = \{\lambda(\alpha^i, \beta\alpha^i, \ldots, \beta^{w-2}\alpha^i) \mid \lambda \in \Phi_w^*\}$, где $i \in \overline{0, n-1}$, $n = \left(w^{m+1} - 1\right)/\left(w - 1\right)$. Из леммы 1 следует, что $A_i \cap A_j = \varnothing$, где $i \ne j$. Действительно, согласно лемме 1 для всех $\alpha^i, \alpha^j \in A$, $i, j \in \overline{0, n-1}$, $i \ne j$, выполняется условие $\beta^r\alpha^i \ne \beta^k\alpha^j$, где $r, k = \overline{0, w-2}$. Обозначим фактор-множество множества $L \setminus \{\bar{0}\}$ по отношению эквивалентности R_D, соответствующее разбиению D, через $PG'(m, w)$. Итак, $PG'(m, w)$ является проективным пространством размерности m над полем Φ_w, индуцированным векторным пространством L над полем Φ_w. Будем говорить, что $PG'(m, w)$ состоит из точек, однородные координаты которых имеют вид: $(\alpha^i) = (\alpha^i : \beta\alpha^i : \ldots : \beta^{w-2}\alpha^i)$, где α — примитивный элемент поля $\Phi_{w^{m+1}}$, $\beta = \alpha^n$, $i = \overline{0, n-1}$, $n = \left(w^{m+1} - 1\right)/\left(w - 1\right)$. Таким образом, верна

Лемма 2. Количество точек в $PG'(m, w)$ равно $n = \left(w^{m+1} - 1\right)/\left(w - 1\right)$.

Рассмотрим произвольное векторное пространство V над некоторым полем k. Назовем каноническим проектированием отображение $\xi : (V \setminus \{\bar{0}\}) \to PG(V)$,

$$\xi(v) = [v], \tag{1}$$

сопоставляющее вектору $v \in V \setminus \{\bar{0}\}$ класс эквивалентности, определенный элементом v [9].

Пусть α — примитивный элемент поля $\Phi_{w^{m+1}}$, где $\Phi_{w^{m+1}} = \Phi_w[x]/\left(f(x)\right)$, $f(x) \in \Phi_w[x]$ — минимальный многочлен α над полем Φ_w. Пусть, $\psi : PG'(m, w) \to PG(m, w)$

$$\psi\left((\alpha^i)\right) = (a_0 : a_1 : \ldots : a_m), \tag{2}$$

где $a_j \in \Phi_w$ — коэффициенты многочлена, являющегося представителем класса эквивалентности, соответствующего α^i в $\Phi_w[x]/\left(f(x)\right)$ с точностью до изоморфизма, $i = \overline{0, n-1}$, $n = \left(w^{m+1} - 1\right)/\left(w - 1\right)$, $j = \overline{0, m}$.

Теорема 1. Отображение Ψ является взаимно однозначным соответствием между множествами $PG^{'}(m,w)$ и $PG(m,w)$. Более того, Ψ отображает проективные подпространства $PG^{'}(m,w)$ на проективные подпространства $PG(m,w)$.

Доказательство. Положим, что $f_i(x)=\sum_{i=0}^{m} a_i x^i$ — представитель класса эквивалентности, соответствующий α^i в $\Phi_w[x]/(f(x))$. Тогда

$$\psi\left((\alpha^i:\beta\alpha^i:\ldots:\beta^{w-2}\alpha^i)_{1\times(w-1)}\right)=(a_0:a_1:\ldots:a_m)_{1\times(m+1)},$$

где $i=\overline{0,n-1}$, $n=\left(w^{m+1}-1\right)/(w-1)$. Легко проверить, что Ψ есть биекция. Действительно, из рассуждений перед леммами 1 и 2 следует, что достаточно проверить инъективность отображения Ψ. Пусть $(a_0:a_1:\ldots:a_m)=(b_0:b_1:\ldots:b_m)$, то есть $b_i=\lambda a_i$, где $i=\overline{0,m}$, $\lambda\in\Phi_w^*$. Поскольку $f_i(x)=\sum_{i=0}^{m} a_i x^i$ и $\lambda f_i(x)=\sum_{i=0}^{m}\lambda a_i x^i$ — представители классов эквивалентности, соответствующие α^j и $\lambda\alpha^j$ в $\Phi_w[x]/(f(x))$, то $\psi\left((\alpha^j)\right)=(a_0:a_1:\ldots:a_m)$ и $\psi\left((\lambda\alpha^j)\right)=(b_0:b_1:\ldots:b_m)$, где $j=\overline{0,n-1}$, $n=\left(w^{m+1}-1\right)/(w-1)$. Но $(\alpha^j)=(\lambda\alpha^j)$ в силу построения $PG^{'}(m,w)$.

Пусть Z — векторное подпространство $\Phi_w[x]/(f(x))$, $\xi(Z\setminus\{\bar{0}\})$ — проективное подпространство $PG(m,w)$. Зафиксируем базис *Z*: $\{t_1,t_2,\ldots,t_k\}$, где $k=dim(Z)$. Тогда точки $\psi^{-1}\left(\xi(t_i)\right)$, где $i=\overline{1,k}$, являются проективно независимыми, то есть, образуют некоторое проективное подпространство $H^{'}\subset PG^{'}(m,w)$: $\xi(Z\setminus\{\bar{0}\})=\psi(H^{'})\cdot$

Таким образом, проективные пространства $PG(m,w)$ и $PG^{'}(m,w)$ над полем Φ_w изоморфны. В дальнейшем вместо $PG^{'}(m,w)$ будем использовать обозначение $PG(m,w)$, отождествляя эти два множества.

Пусть α — примитивный элемент поля $\Phi_{w^{m+1}}$, $\beta=\alpha^n$, где $n=\left(w^{m+1}-1\right)/(w-1)$. Рассмотрим отображение $\tau:\Phi^*_{w^{m+1}}\to PG(m,w)$,

$$\tau(\alpha^i\beta^j)=(\alpha^i),\tag{3}$$

где $i\in\overline{0,n-1}$, $j\in\overline{0,w-2}$. Из леммы 1 легко увидеть, что верна

Лемма 3. Отображение τ является сюръективным.

Пусть α — примитивный элемент поля $\Phi_{w^{m+1}}$, $\beta=\alpha^n$, где $n=\left(w^{m+1}-1\right)/(w-1)$. Рассмотрим произвольное конечное поле Φ_{p^z}, где p^z — положительная степень некоторого простого числа $p,z\in\mathrm{N}$, $p^z\le w^{m+1}$, *d* — примитивный элемент поля Φ_{p^z}. Рассмотрим отображение $\mu:\Phi^*_{p^z}\to\Phi^*_{w^{m+1}}$,

$$\mu(d^y)=\alpha^y,\tag{4}$$

где $y\in\overline{0,p^z-2}$. Очевидно, что μ является инъективным отображением. Заметим, что любой элемент $a\in\Phi^*_{w^{m+1}}$ может быть единственным образом представлен в виде $a=\alpha^i\beta^j$, где $i\in\overline{0,n-1}$, $j\in\overline{0,w-2}$. Определим отображение $\delta:\Phi^*_{p^z}\to\Phi^*_w$,

$$\delta(b)=\beta^j,\tag{5}$$

где $\mu(b)=\alpha^i\beta^j$ для некоторых $i\in\overline{0,n-1}$, $j\in\overline{0,w-2}$.

Рассмотрим произвольное конечное поле Φ_{p^z}, где *p* — простое число, $z\in\mathrm{N}$, $p^z\le w^{m+1}$. Определим отображение $\phi:\Phi^*_{p^z}\to PG(m,w)\times\to\Phi^*_w$

$$\phi(b)=\left(\tau(\mu(b)),\delta(b)\right),\tag{6}$$

где используются ранее определенные отображения τ (3), μ (4), δ (5). Из лемм 1 и 3 легко увидеть, что верна

Теорема 2. Отображение ϕ является инъективным.

Вернемся к описанию разработанного алгоритма. Покажем, как сопоставить секрету точку проективного пространства. Секретный ключ x представляет собой элемент мультипликативной группы Z_q^*, где q — простое число, так что $x \in \overline{1, q-1}$. Для генерации секрета зафиксируем случайный порождающий элемент b циклической группы Z_q^* и некоторое целое число $i \in \overline{0, q-2}$, а затем положим $b^i = x$. Далее зафиксируем примитивный элемент α поля $\Phi_{w^{m+1}}$. Поскольку $q < w^{m+1}$, то можно рассмотреть ранее определенное инъективное отображение $\mu : Z_q^* \to \Phi_{w^{m+1}}^*$ (4). Итак, $\mu(b^i) = \alpha^i$, где $i \in \overline{0, q-2}$. Поскольку можно легко вычислить элемент α^n, где $n = \left(w^{m+1} - 1\right)/\left(w - 1\right)$, то $\alpha^i = \alpha^{vn+r}$, где $v \in Z$, $r \in N$, согласно алгоритму Евклида. Таким образом, используя отображение $\tau : \Phi_{w^{m+1}}^* \to PG(m, w)$ (3) получаем $\tau(\alpha^i) = \tau(\alpha^{vn+r}) = (\alpha^r)$. Также, исходя из определения $\delta : Z_q^* \to \Phi_w^*$ (5), вычисляем $\delta(b^i) = \alpha^{vn}$. Следовательно, отображение $\phi : Z_q^* \to PG(m, w) \times F_w^*$ (6) сопоставляет секретному ключу $\phi(x) = \left((\alpha^r), \alpha^{vn}\right)$. Публикуем значение $v \in Z$. Случайным образом строим проективную прямую $l \in PG(m, w)$: $(\alpha^r) \in l$. Полученная проективная прямая l публикуется. Итак, будем обозначать «секретную» точку, то есть точку, которая сопоставляется секрету при помощи отображения ϕ, через $(c) \in PG(m, w)$.

Далее администратор генерирует систему попарно различных проективных подпространств $\{M_i\}_{i=1}^N \subset PG(m, w)$ размерности $t-1$, таких что $M_i \cap l = (c)$, где $i = \overline{1, N}$, N — количество команд проверяющих. Так как число людей в одной команде $2 \le t \le m$, то размерность d создаваемых проективных подпространств в зависимости от t может принимать значения $1 \le d \le m-1$, то есть создаваемое проективное пространство может быть некоторой проективной прямой в случае $t = 2$, а при $t = m$ — проективной гиперплоскостью в $PG(m, w)$.

Пусть одним из построенных проективных подпространств будет $M' \subset PG(m, w)$. Пусть M есть t-мерное векторное подпространство векторного пространства $\Phi_{w^{m+1}}$ над полем Φ_w, для которого выполняется условие $\xi(M) = M'$, где ξ — ранее определенное каноническое проектирование (1). Рассмотрим максимальный флаг длины t, получаемый при помощи базисных векторов M $\{\beta_1, \beta_2, \ldots, \beta_t\} \subset \Phi_{w^{m+1}}$: $M_0 = \langle \overline{0} \rangle \subset M_1 = \langle \beta_1 \rangle \subset \ldots \subset M_t = \langle \beta_1, \beta_2, \ldots, \beta_t \rangle$. Тогда для «секретной» точки $(c) \in PG(m, w)$ и элемента $c' \in \Phi_{w^{m+1}}$: $\xi(c') = (c)$, должно выполняться условие $c' \in M_t \setminus M_{t-1}$. Необходимость соблюдения этого условия будет ясна из дальнейших рассуждений.

Существует несколько способов сгенерировать искомое $(t-1)$-мерное проективное подпространство $M' \subset PG(m, w)$. Опишем один из таких методов, который заключается в переходе от одного базиса к другому.

Зафиксируем некоторый базис $\beta = \{\beta_1, \beta_2, \ldots, \beta_{m+1}\}$ векторного пространства $\Phi_{w^{m+1}}$ над полем Φ_w. Рассмотрим разложение элемента $c \ne 0$, $c \in \Phi_{w^{m+1}}$ по этому базису: $c = \sum_{i=1}^{m+1} v_i \beta_i$, где $v_i \in \Phi_w$. Пусть в этом разложении ровно $j \in \overline{1, m+1}$ коэффициентов $v_{k_1}, v_{k_2}, \ldots, v_{k_j}$ отличны от нуля, где $k_i \in \overline{1, m+1}$, $i = \overline{1, j}$. Перенумеруем элементы базиса β так, что для нового базиса β^j выполняется условие: $\beta_i^j := \beta_{k_i}$ и $l_i^j := l_{k_i}$, где $i = \overline{1, j}$, то есть в разложении c по базису β^j все коэффициенты отличные от нуля находятся на первых j позициях: $c = \sum_{i=1}^{j} l_i^j \beta_i^j = \sum_{i=1}^{m+1} v_i \beta_i$. Заметим, что в качестве такого начального базиса β удобнее всего выбрать полиномиальный базис, в силу построения $PG(m, w)$.

Если для рассматриваемого базиса β^j выполняется условие: $j = t$, то достигли желаемого результата.

Пусть $1 \le j \le t-1$. Зафиксируем некоторый элемент $l_{j+1}^{j+1} \in \Phi_w^*$. Приведем пример матрицы перехода $A_{j+1} \in GL_{m+1}(\Phi_w)$ от j-го базиса $\{\beta_i^j\}_{i=1}^{m+1}$ к $(j+1)$-му $\{\beta_i^{j+1}\}_{i=1}^{m+1}$ базису векторного пространства $\Phi_{w^{m+1}}$ над полем Φ_w, такому что $c = \sum_{i=1}^{j+1} l_i^{j+1}\beta_i^{j+1}$, где $l_i^{j+1} = l_i^j$, $i = \overline{1, j}$, $\beta_k^{j+1} = \beta_k^j$, где $k = \overline{1, m+1}$, $k \notin \overline{j, j+1}$, $\beta_j^{j+1} = \beta_j^j - \frac{\eta l_{j+1}^{j+1}}{l_j^{j+1}}\beta_{j+1}^j$, $\beta_{j+1}^{j+1} = \eta\beta_{j+1}^j$, где $\eta \in \Phi_w^*$ — произвольный, но зафиксированный, элемент. Пусть $\beta_v^{j+1} = (\beta_1^{j+1}, \beta_2^{j+1}, \ldots, \beta_{m+1}^{j+1})^T$, $\beta_v^j = (\beta_1^j, \beta_2^j, \ldots, \beta_{m+1}^j)^T$. Матрица A_{j+1}: $\beta_v^{j+1} = A_{j+1}\beta_v^j$, представляет собой единичную матрицу, за тем исключением что в ее $j+1$ столбце единственными ненулевыми элементами являются $a_{j,j+1} = -\frac{\eta l_{j+1}^{j+1}}{l_j^{j+1}}$ и $a_{j+1,j+1} = \eta$, находящиеся в j-ой и $(j+1)$-ой строках соответственно. Тогда $\beta_j^{j+1} = \beta_j^j - \frac{\eta l_{j+1}^{j+1}}{l_j^{j+1}}\beta_{j+1}^j$, $\beta_{j+1}^{j+1} = \eta\beta_{j+1}^j$ и $\beta_k^{j+1} = \beta_k^j$, где $k = \overline{1, m+1}$, $k \notin \overline{j, j+1}$. Таким образом, проделывая описанную процедуру $t-j$ раз, начиная с базиса β^j, получаем базис $\beta^t = \{\beta_1^t, \beta_2^t, \ldots, \beta_{m+1}^t\}$ векторного пространства $\Phi_{w^{m+1}}$ над полем Φ_w: $c = \sum_{i=1}^{t} l_i^t\beta_i^t$, где $l_i^t \in \Phi_w^*$, $i = \overline{1, t}$.

Пусть $t+1 \le j \le m+1$. Опишем матрицу перехода $B_{j-1} \in GL_{m+1}(\Phi_w)$ от j-го базиса $\{\beta_i^j\}_{i=1}^{m+1}$ к $(j-1)$-му $\{\beta_i^{j-1}\}_{i=1}^{m+1}$ базису векторного пространства $\Phi_{w^{m+1}}$ над полем Φ_w, такому что $c = \sum_{i=1}^{j-1} l_i^{j-1}\beta_i^{j-1}$, где $l_i^{j-1} = l_i^j$, $i = \overline{1, j-1}$, $\beta_k^{j-1} = \beta_k^j$, где $k = \overline{1, m+1}$, $k \notin \overline{j-1, j}$, $\beta_{j-1}^{j-1} = \beta_{j-1}^j + \frac{l_j^j}{l_{j-1}^{j-1}}\beta_j^j$, $\beta_j^{j-1} = \frac{\beta_j^j}{\eta}$, где $\eta \in \Phi_w^*$ — произвольный, но зафиксированный, элемент. Пусть $\beta_v^{j-1} = (\beta_1^{j-1}, \beta_2^{j-1}, \ldots, \beta_{m+1}^{j-1})^T$, $\beta_v^j = (\beta_1^j, \beta_2^j, \ldots, \beta_{m+1}^j)^T$. Матрица B_{j-1}: $\beta_v^{j-1} = B_{j-1}\beta_v^j$, представляет собой единичную матрицу, за тем исключением что в ее j столбце единственными ненулевыми элементами являются $b_{j-1,j} = \frac{l_j^j}{l_{j-1}^{j-1}}$ и $b_{j,j} = \frac{1}{\eta}$, находящиеся в $(j-1)$-ой и j-ой строках соответственно. Тогда $\beta_{j-1}^{j-1} = \beta_{j-1}^j + \frac{l_j^j}{l_{j-1}^{j-1}}\beta_j^j$, $\beta_j^{j-1} = \frac{\beta_j^j}{\eta}$ и $\beta_k^{j-1} = \beta_k^j$, где $k = \overline{1, m+1}$, $k \notin \overline{j-1, j}$. Таким образом, проделывая описанную процедуру $j-t$ раз, начиная с базиса β^j, получаем базис $\beta^t = \{\beta_1^t, \beta_2^t, \ldots, \beta_{m+1}^t\}$ векторного пространства $\Phi_{w^{m+1}}$ над полем Φ_w: $c = \sum_{i=1}^{t} l_i^t\beta_i^t$, где $l_i^t \in \Phi_w^*$, $i = \overline{1, t}$.

Таким образом, если $c' \in \Phi_{w^{m+1}}$: $\xi(c') = (c)$, где $(c) \in PG(m, w)$ — «секретная» точка, ξ — отображение (1), то, применяя вышеописанный метод, находим базис $\beta^t = \{\beta_1^t, \beta_2^t, \ldots, \beta_{m+1}^t\}$ векторного пространства $\Phi_{w^{m+1}}$ над полем Φ_w: $c' = \sum_{i=1}^{t} l_i^t\beta_i^t$, где $l_i^t \in \Phi_w^*$, $i = \overline{1, t}$. Отсюда можно построить t-мерное векторное подпространство $M = \left\langle \beta_1^t, \beta_2^t, \ldots, \beta_t^t \right\rangle \subset \Phi_{w^{m+1}}$: $c' \in M_t \setminus M_{t-1}$, где $M_{t-1} = \left\langle \beta_1^t, \beta_2^t, \ldots, \beta_{t-1}^t \right\rangle$, $M_t = M$. Рассмотрим линейно независимые элементы y и c' векторного пространства $\Phi_{w^{m+1}}$ над полем Φ_w, причем $y \notin M$. Зафиксируем двумерное подпространство $l' = \left\langle c', y \right\rangle \subset \Phi_{w^{m+1}}$. Тогда проективно независимые точки $\xi(\beta_i^t) \in PG(m, w)$, где $i = \overline{1, t}$, являются секретными долями, раздаваемые одной из команд, а проективная прямая $\xi(l') = l \subset PG(m, w)$ – частью открытого ключа, где ξ — ранее определенное каноническое проектирование (1).

Открытый ключ. Открытый ключ состоит из последовательности $(p, g, y = g^x)$, где p — простое число, g — порождающий элемент мультипликативной абелевой группы $G \subset Z_p^*$, причем порядок группы $Ord(G) = q$, где q — такое простое число, что $q = (p-1)/2$, x — секретный ключ: $x \in \overline{1, q-1}$. Также параметрами открытого ключа являются α — примитивный элемент поля $\Phi_{w^{m+1}}$, пара (w, m), где w — положительная степень некоторого простого числа, $m \in \mathrm{N}$, проективная прямая $l \subset PG(m, w)$, которой принадлежит «секретная» точка, целое число $v \in \mathrm{Z}$, используемое при восстановлении секрета, описание инъективного отображения $\rho : \Phi_r^z \to G$, где $r^z < q$, r — простое число, $z \in \mathrm{N}$ — число кандидатов.

Этап голосования и шифрования «голоса». Пусть выборы проходят по следующим правилам: 1. всего участвуют $z \in \mathrm{N}$ кандидатов; 2. проголосовать можно только за одного кандидата. Все голоса будут представлять собой некоторые элементы векторного пространства Φ_r^z над полем Φ_r, где r — простое число (см. описание строения открытого ключа). Поскольку $r^z < q$, то можно построить инъективное отображение из Φ_r^z в G, которое будем обозначать через $\rho : \Phi_r^z \to G$. Положим, что избиратель проголосовал за i-го кандидата, где $i = \overline{1, z}$. Тогда $\overline{u} = (a_1, a_2, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_z) \in \Phi_r^z$, где $a_j \in \Phi_r$: $a_j \neq 1$, $j = \overline{1, z}$, $j \neq i$, является открытым текстом. Далее происходит сопоставление вектору $\overline{u}$ некоторого элемента $h \in G$: $\rho(\overline{u}) = h$. Затем избиратель генерирует произвольное число $k \in \overline{1, q-1}$, равномерно распределенное в Z_q^*, и на основе публичного ключа применяет отображение $E : G^2 \to G^2$, $E(k, h) = (g^k, y^k h)$, задающее шифрование по схеме Эль-Гамаля. $E(k, z)$ является шифротекстом, который отправляется проверяющим.

Этап дешифрования «голоса». Все множество голосов можно разбить среди N команд, чтобы уменьшить время подсчета голосов.

Определим отображение $D : G^2 \to G$, $D\left((g^k, y^k h)\right) = g^{-xk} y^k h = h$, задающее дешифрование по схеме Эль-Гамаля, где x — секретный ключ.

Перед тем как расшифровать полученные шифротексты проверяющим понадобится восстановить секретный ключ $x \in \overline{1, q-1}$. Пусть какая-то из команд S_i, где $i = \overline{1, N}$, пытается восстановить x. Для этого каждый из участников $s_{ij} \in S_i$ публикует свою секретную долю $(\beta_{ij}) \in PG(m, w)$, где $j = \overline{1, t}$. Прямая сумма системы проективно независимых точек $\{(\beta_{ij})\}_{j=1}^t$ равна проективному подпространству $M_i \subset PG(m, w)$: $M_i \cap l = (c)$, где $l \subset PG(m, w)$ — известная проективная прямая, (c) — «секретная» точка. Опишем один из способов нахождения данного пересечения.

Пусть $\{\beta_1, \beta_2, \ldots, \beta_{m+1}\}$ — базис векторного пространства $\Phi_{w^{m+1}}$ над полем Φ_w, построенный на этапе генерации секретных долей. Тогда $M = \langle \beta_1, \beta_2, \ldots, \beta_t \rangle$ — векторное подпространство $\Phi_{w^{m+1}}$ над полем Φ_w: $\xi(M)$ — проективное подпространство $PG(m, w)$, равное прямой сумме секретных долей. Рассмотрим двумерное векторное подпространство $l' \subset \Phi_{w^{m+1}}$, такое что $\xi(l') = l \subset PG(m, w)$, где l — известная из публичного ключа проективная прямая, содержащая «секретную» точку. Векторное подпространство, получаемое в результате пересечения $M \cap l'$, должно быть одномерным подпространством векторного пространства $\Phi_{w^{m+1}}$ над полем Φ_w. Зафиксируем некоторое множество базисных векторов $\{y, h\}$, порождающих подпространство $l' = \langle y, h \rangle$, где y, $h \in \Phi_{w^{m+1}}$. Следовательно, не нарушая общность рассуждений, можно положить, что $y \notin M$, а координата вектора y: $y_{t+1} \in \Phi_w^*$. Для вектора, принадлежащего $v \in M \cap l'$, выполняется условие: $v = \sum_{i=1}^t v_i \beta_i = \lambda_1 y + \lambda_2 h$, где λ_1, $\lambda_2 \in \Phi_w$. Таким образом, для нахождения пересечения необходимо решить следующую систему линейных уравнений:

$$\begin{pmatrix} -1 & 0 & \cdots & 0 & y_1 & h_1 \\ 0 & -1 & \cdots & 0 & y_2 & h_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & y_t & h_t \\ 0 & 0 & \cdots & 0 & y_{t+1} & h_{t+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & y_{m+1} & h_{m+1} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_t \\ \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Ранг данной матрицы должен равняться $t+1$, что возможно тогда и только тогда, когда $\left(y_{t+1}h_i - y_i h_{t+1}\right)/\, y_{t+1} = 0$, $i \in \overline{t+2, m+1}$. Легко увидеть, что если A — линейное отображение, соответствующее матрице данной СЛАУ, то

$$x \in ker(A) \Leftrightarrow x = \lambda_2 \begin{pmatrix} \dfrac{y_{t+1}h_1 - y_1 h_{t+1}}{y_{t+1}} & \dfrac{y_{t+1}h_2 - y_2 h_{t+1}}{y_{t+1}} & \cdots & \dfrac{y_{t+1}h_t - y_t h_{t+1}}{y_{t+1}} & -\dfrac{h_{t+1}}{y_{t+1}} & 1 \end{pmatrix}^T,$$

где $\lambda_2 \in \Phi_{w}$. Рассмотрим элемент $x' = \sum_{i=1}^{t} \dfrac{y_{t+1}h_i - y_i h_{t+1}}{y_{t+1}} \beta_i = \alpha^s \in \Phi_{w^{m+1}}$, α — примитивный элемент поля $\Phi_{w^{m+1}}$, $s \in \overline{0, w^{m+1} - 2}$. Итак, $x' = \alpha^s = \alpha^r \alpha^{nl}$, где $r \in \overline{0, n-1}$, $n = \left(w^{m+1} - 1\right)/\left(w-1\right)$, $l \in \mathrm{Z}$. Следовательно, при помощи отображения τ (3) получаем $\tau(x') = \tau(\alpha^r \alpha^{nl}) = (\alpha^r) \in PG(m,w)$ — «секретную» точку. Далее применяем левое обратное отображение $\varphi^{-1} : PG(m,w) \times \Phi_w^* \to \mathrm{Z}_q^*$ к (6), и — $\mu^{-1} : \Phi_{w^{m+1}}^* \to \mathrm{Z}_q^*$ к (4), а также известное из публичного ключа $v \in \mathrm{Z}$: $\varphi^{-1}\left((\alpha^r), \alpha^{nv}\right) = \mu^{-1}(\alpha^r \alpha^{nv}) = \mu^{-1}(\alpha^i) = b^i = x$, где $i \in \overline{0, q-2}$, b — порождающий элемент Z_q^*, x — секретный ключ.

Предположим, что необходимо расшифровывать шифротекст $E(k,h) \in G^2$. Для этого используем отображение $D\left(E(k,h)\right) = h \in G$. Для того чтобы восстановить вектор $\bar{u} \in \Phi_r^z$, являющийся открытым текстом, применим отображение $\gamma^{-1} : G \to \Phi_r^z$, которое является левым обратным к общеизвестному инъективному отображению γ, то есть $\gamma^{-1}(h) = \bar{u}$.

Определение результатов голосования. Пусть $U = \{\bar{u}_i\}_{i=1}^{d} \subset \Phi_r^z$ — множество всех «голосов», где $d \in \mathrm{N}$, $\lambda : \Phi_r^z \to \Phi_r^z$, $\lambda(\bar{u}) = (0,0,\ldots,0,1_i,0,\ldots,0)$, если i-й элемент вектора $\bar{u}$ равен 1, $i \in \overline{1,z}$. После дешифрования «голосов» находим вектор $\bar{R} = \sum_{i=1}^{d} \lambda(\bar{u}_i) \in \mathrm{Z}^z$, где j-ый элемент $\bar{R}$ в силу предыдущих рассуждений представляет собой количество голосов за j-го кандидата, $j \in \overline{1,z}$. Вектор $\bar{R}$ публикуется и объявляется результатом выборов.

Теорема 3. Если злоумышленнику известно множество проективных точек $U \subset PG(m,w)$, являющихся секретными долями, где $|U| \le t-1$, то вероятность того, что он правильно сгенерирует «секретную» точку равна $1/(w+1)$.

Доказательство. Поскольку злоумышленнику известна проективная прямая $l \subset PG(m,w)$, которой принадлежит искомая «секретная» точка (c), то вероятность сгенерировать верную «секретную» точку перед началом каких-либо преобразований равна $1/(w+1)$. Действительно, произвольная проективная прямая, принадлежащая $PG(m,w)$, содержит $w+1$ точек. Имея в своем распоряжении публичный ключ, злоумышленник знает элемент $v \in \mathrm{Z}$: $c' = \alpha^i \alpha^{vn}$, где $\tau(c') = \tau(\alpha^i \alpha^{vn}) = (\alpha^i) = (c)$ (3), $i \in \overline{0, n-1}$, $n = \left(w^{m+1} - 1\right)/\left(w-1\right)$. Но в силу построения сюръективного отображения τ для любого из n элементов вида α^j, где $j \in \overline{0, n-1}$, $\tau(\alpha^j \alpha^{vn}) = (\alpha^j)$, то есть вероятность сгенерировать верный «секретный» ключ по элементу $\alpha^{vn} \in \Phi_w^*$ равна $1/n = (w-1)/(w^{m+1} - 1)$. Пусть злоумышленник, используя проективно независимые точки, из которых состоит множество $U \subset PG(m,w)$, строит проективное подпространство $W \subset PG(m,w)$, размерность

которого строго меньше $t-1$. Поскольку при восстановлении «секретной» точки ищется прямая сумма всех секретных долей, то проективное подпространство W не пересекается с проективной прямой l в силу построения множества U. Итак, злоумышленнику известно, что искомая «секретная» точка не принадлежит U. Для любой точки $(s) \in l$ проективное подпространство $\langle U \cup (s) \rangle \subset PG(m, w)$ имеет размерность меньшую либо равную $t-1$. Тогда вероятность того, что (s) является искомой точкой, равна $1/(w+1)$.

Выводы. В работе описан разработанный авторами способ организации электронных выборов, в основе которых лежит использование схемы Эль-Гамаля и метода порогового разделения секрета, опирающегося на свойства проективных пространств, заданных над конечными полями. Построен полиномиальный детерминированный алгоритм, криптографическая стойкость которого опирается на общепризнанно трудноразрешимую проблему Диффи-Хеллмана в конечном поле [10]. Доказано, что предложенные методы позволяют защитить передаваемые от нечестных проверяющих данные за счет особенности способа генерации секретных долей, представляющих собой точки некоторого проективного пространства. Таким образом, определена вероятность создания злоумышленником верной секретной доли при условии, что ему известна лишь некоторая часть секретных долей.

Библиографический список

1. Могилевская, Н. С. Пороговое разделение файлов на основе битовых масок: идея и возможное применение / Н. С. Могилевская, Р. В. Кульбикаян, Л. А. Журавлев // Вестник Дон. гос. техн. ун-та. — 2011 — Т. 11, 10. — С. 1749–1755.

2. Rubin, A. D. Security considerations for remote electronic voting / A. D. Rubin // Communications of the ACM. – 2002. – V. 45(12). – P. 39–44.

3. Kiayias, A. An Internet voting system supporting user privacy / A. Kiayias, M. Korman, D. Walluck // ACSAC'06: Proceedings of the 22nd Annual Computer Security Applications Conference. – 2006. – P. 165–174.

4. Jefferson, D. Analyzing internet voting security / D. Jefferson, A. D. Rubin, B. Simons, D. Wagner // Communications of the ACM. – 2004. – V. 47(10). – P. 59–64.

5. Chaum, D. Secret-ballot receipts: True voter-verifiable elections / D. Chaum // IEEE Security and Privacy. – 2004. – V. 2(1). – P. 38–47.

6. Алферов, А. П. Основы криптографии: учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. — Москва : Гелиос-АРВ, 2001. — 480 с.

7. Рябко, Б. Я. Криптографические методы защиты информации / Б. Я. Рябко, А. Н. Фионов. — Москва : Горячая линия-Телеком, 2005. — 229 с.

8. Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц. — Москва : ТВП, 2001. — 254 с.

9. Кострикин, А. И. Введение в алгебру / А. И. Кострикин. — Москва : МЦНМО, 2009. — 368 с.

10. Ian, F. Blake. On the complexity of the discrete logarithm and Diffie-Hellman problems / F. Blake Ian, Theo Garefalakis // J. Complex. – 2004. – V. 20(2-3). – P. 148–170.

References

1. Mogilevskaya, N.S., Kulbikayan, R.V., Zhuravlev, L.A. Porogovoe razdelenie faylov na osnove bitovykh masok: ideya i vozmozhnoe primenenie. [Threshold file sharing based on bit masks: concept and possible use.] Vestnik of DSTU, 2011, vol. 11, no. 10, pp. 1749–1755 (in Russian).

2. Rubin, A. D. Security considerations for remote electronic voting. Communications of the ACM, 2002, vol. 45(12), pp. 39–44.

3. Kiayias, A., Korman, M., Walluck, D. An Internet voting system supporting user privacy. ACSAC'06: Proceedings of the 22nd Annual Computer Security Applications Conference, 2006, pp. 165–174.

4. Jefferson, D., Rubin, A. D., Simons, B., Wagner, D. Analyzing internet voting security. Communications of the ACM, 2004, vol. 47(10), pp. 59–64.

5. Chaum, D. Secret-ballot receipts: True voter-verifiable elections. IEEE Security and Privacy, 2004, vol. 2(1), pp. 38–47.

6. Alferov, A.P., Zubov, A.Yu., Kuzmin, A.S., Cheremushkin, A.V. Osnovy kriptografii: uchebnoe posobie. [Basics of Cryptography.] Moscow: Gelios-ARV, 2001, 480 p. (in Russian).

7. Ryabko. B.Ya., Fionov, A.N. Kriptograficheskie metody zashchity informatsii. [Cryptographic methods of information protection.] Moscow: Hot line -Telekom, 2005, 229 p. (in Russian).

8. Koblitz, N. Kurs teorii chisel i kriptografii. [Course of number theory and cryptography.] Moscow: TVP, 2001, 254 p. (in Russian).

9. Kostrikin, A.I. Vvedenie v algebru. [Introduction to Algebra.] Moscow: MTsNMO, 2009, 368 p. (in Russian).

10. Ian, F. Blake, Garefalakis, Theo. On the complexity of the discrete logarithm and Diffie-Hellman problems. J. Complex, 2004, vol. 20(2-3), pp. 148–170.

Поступила в редакцию 06.12.2017
Сдана в редакцию 07.12.2017
Запланирована в номер 15.03.2018

Received 06.12.2017
Submitted 06.12.2017
Scheduled in the issue 17.03.2018

Об авторах:

Мазуренко Александр Вадимович,
математик-программист ООО "ДДОС-Гвард"
(РФ, 344002, Ростов-на-Дону, пр. Буденовский, 62/2)
ORCID: https://orcid.org/0000-0001-9541-3374
mazurencoal@gmail.com

Стукопин Владимир Алексеевич,
и.о. зав. каф. «Математика» Донского государственного технического университета (РФ, 344000, г. Ростов-на-Дону, пл. Гагарина, 1), доктор физико-математических наук, доцент
ORCID: https://orcid.org/0000-0001-9911-8962
stukopin@mail.ru

Authors:

Mazurenko, Alexander V.,
mathematician-programmer, DDoS-GUARD LLC (RF, 344002, Rostov-on-Don, Budenovskiy pr. 62/2)
ORCID: https://orcid.org/0000-0001-9541-3374
mazurencoal@gmail.com

Stukopin, Vladimir A.,
acting head of the Mathematics Department, Don State Technical University (RF, 344000, Rostov-on-Don, Gagarin sq., 1), Dr.Sci. (Phys.-Math.), associate professor
ORCID: https://orcid.org/0000-0001-9911-8962
stukopin@mail.ru